Autenticación Multifactor

Las técnicas expuestas a continuación suelen ser utilizadas por los bancos para incrementar el nivel de seguridad de sus sistemas. Suelen denominarse segundo factor autenticación o autenticación multifactor y se utilizan para operar en banca digital en alguno de sus formatos, como cajeros automáticos, *home banking*, tarjetas de crédito, etc.

Clave alfabética

La llamada identificación alfabética o clave alfabética es una técnica de seguridad que permite validar operaciones como extracciones y transferencias en cajeros automáticos dificultando accesos no autorizados. En algunos casos reemplaza la validación de 3 dígitos del DNI. Estas claves se generan en el propio cajero eligiendo 3 letras en orden, seleccionando de entre 8 grupos de opciones como se muestra en la figura 1. Al ser solicitada esa clave de 3 letras para validar una operación hay que seleccionarlas nuevamente de los 8 grupos en pantalla.

Figura 1: Ejemplo de clave alfabética

Validación de operaciones bancarias mediante tres dígitos del DNI

Hace un tiempo, para validar algunas operaciones bancarias realizadas en cajeros automáticos, se pedía a modo de segundo factor de autenticación, seleccionar de entre una cantidad de opciones tres dígitos consecutivos del Documento Nacional de Identidad (DNI), que podía corresponder al grupo de unidades a centenas, o de unidades de mil a centenas de mil. Esta estrategia se reemplazó luego por otras como la clave alfabética.

Tarjeta de coordenadas

La tarjeta de coordenadas es otra herramienta de seguridad adicional al PIN (número de identificación personal) o clave de seguridad bancaria requerida para realizar ciertas operaciones. Puede considerarse como una forma de OTP (*One Time Password*). Como es un mecanismo dinámico, es más difícil robar claves para autenticarse, porque cada vez que se utilice se necesitará una coordenada distinta, que es aleatoria y vence con cada sesión. Actualmente existen sistemas

más seguros que las tarjetas de coordenadas, como por ejemplo el *token*. Estas tarjetas son (o eran) de plástico, del tamaño de una tarjeta de crédito, con una matriz o cuadrícula de números impresos, es decir, ordenados en filas y columnas. Cada uno de estos números podía ser de dos o tres dígitos. Se usaron tarjetas de coordenadas de 9 por 9 y de 10 por 10 casilleros. En la figura 2 puede verse un ejemplo de Tarjeta de Coordenadas.

Figura 2: Ejemplo de tarjeta de coordenadas

Para activar las tarjetas de coordenadas había que acudir a un cajero automático, introducir la tarjeta de débito y el PIN correspondiente, naturalmente seleccionar una opción de Asociación de Tarjeta Coordenadas o similar, y seguir los pasos que se indicaban en pantalla entre los que estaba introducir un número de serie, también impreso en la tarjeta. Una vez finalizada esta operación, la Tarjeta de Coordenadas estaba lista para ser utilizada y para realizar operaciones se solicitaba el ingreso del número en una de las coordenadas.

Token

Es otra técnica usada como segundo factor de autenticación para *home banking* que permite tener una clave adicional para validar las operaciones cursadas por estos canales. Es una forma de OTP (*One Time Password*). Típicamente reemplazó a la tarjeta de coordenadas. El sistema generador de estas claves está incluido en las aplicaciones de *home banking* antes del inicio de sesión, o bien en una aplicación aparte. Es decir, que es necesario instalar una aplicación auténtica en el teléfono inteligente.

En algunos bancos, cuando se está realizando una operación que requiera validación adicional, y antes de finalizar la misma, el sistema solicitará el ingreso del *Token*. Para ello, se debe ingresar en la aplicación, y buscar la opción Token. El código mostrado en el teléfono debe ingresarse para confirmar y finalizar la operación.

Se suele requerir que la hora del teléfono configurada en modo "automático", y es importante saber qué hacer ante pérdida o robo del teléfono.

Validación a través de camino alternativo

Es una contraseña alfanumérica (es decir, puede tener letras, números y caracteres especiales) que el sistema envía al usuario a través de mensajería, correo electrónico o una llamada telefónica de manera instantánea, y se solicita al usuario que la ingrese para completar la operación. Se emplea

para validar operaciones como transferencias o compras *online*, entre otras. En casos de seguridad más fuertes incluso se utiliza para validar el inicio de sesión.